

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2000-99403

(P2000-99403A)

(43)公開日 平成12年4月7日(2000.4.7)

(51)Int.Cl.<sup>7</sup>

G 0 6 F 12/14

識別記号

3 2 0

3 1 0

F I

G 0 6 F 12/14

テーマコード(参考)

3 2 0 B 5 B 0 1 7

3 1 0 K

審査請求 未請求 請求項の数26 O L (全 11 頁)

(21)出願番号 特願平10-265210

(22)出願日 平成10年9月18日(1998.9.18)

(71)出願人 000003223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72)発明者 小谷 誠剛

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(72)発明者 長谷部 高行

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(74)代理人 100094145

弁理士 小野 山己男 (外2名)

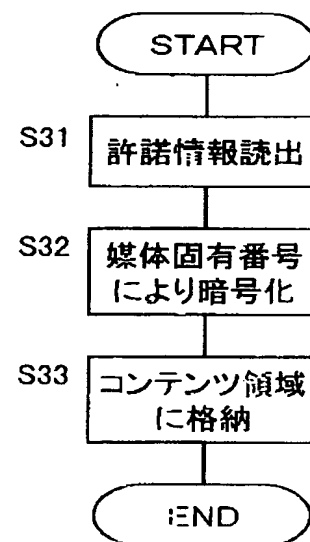
最終頁に続く

(54)【発明の名称】 情報管理方法および情報管理装置

(57)【要約】

【課題】 記録媒体上に格納された電子化データを利用するために必要な許諾情報がなんらかの障害により破壊された場合であっても、ユーザがバックアップ情報を用いてこれを復帰させることが可能な情報管理方法を提供する。

【解決手段】 記録媒体のユーザによるアクセスが不可能な第2階層に格納されている許諾情報を読み出して(ステップS31)、記録媒体の媒体固有番号によって暗号化し(ステップS32)、暗号化した許諾情報を記録媒体のユーザが任意に利用できる第3階層に格納する(ステップS33)。



## 【特許請求の範囲】

【請求項1】媒体固有の情報を有する記録媒体上の所定の領域に格納された所定の情報を、前記媒体固有の情報またはそれに基づいて生成された鍵により暗号化して前記所定の領域外に導出する情報管理方法。

【請求項2】前記記録媒体は、前記所定の情報を格納する第1領域と、前記第1領域と異なる第2領域とを備える、請求項1に記載の情報管理方法。

【請求項3】前記第2領域は外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域であり、前記第1領域は外部からの指令に基づいて制御することが不可能な機密領域である、請求項2に記載の情報管理方法。

【請求項4】前記第2領域に格納される任意の情報は暗号化された電子化データであり、前記第1領域に格納される所定の情報は前記電子化データを利用する利用権に基づく許諾情報を含む、請求項3に記載の情報管理方法。

【請求項5】前記所定の情報は、前記媒体固有の情報またはそれに基づいて生成された鍵により暗号化されて前記所定の領域に格納されている、請求項2～4のいずれかに記載の情報管理方法。

【請求項6】前記所定の情報は、前記記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化されている、請求項5に記載の情報管理方法。

【請求項7】前記暗号化された所定の情報を前記第2領域に格納する、請求項2～6のいずれかに記載の情報管理方法。

【請求項8】前記第2領域に格納されている暗号化された所定の情報を前記媒体固有の情報またはそれに基づいて生成された鍵により復号化し、前記第1領域に格納されている所定の情報を更新する、請求項7に記載の情報管理方法。

【請求項9】前記所定の情報を前記第1領域外に導出する際に、前記媒体固有の情報またはそれに基づいて生成された鍵および前記記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項7に記載の情報管理方法。

【請求項10】前記第2領域に格納されている暗号化された所定の情報を、前記記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して、前記第1領域に格納されている所定の情報を更新する、請求項9に記載の情報管理方法。

【請求項11】前記暗号化された所定の情報を、前記記録媒体とは異なる第2の記録媒体上に格納する、請求項1～6のいずれかに記載の情報管理方法。

【請求項12】前記第2の記録媒体に格納されている暗号化された所定の情報を前記媒体固有の情報またはそれ

に基づいて生成された鍵により復号化し、前記所定の領域に格納されている所定の情報を更新する、請求項11に記載の情報管理方法。

【請求項13】前記所定の情報を前記第2の記録媒体上に導出する際に、前記媒体固有の情報またはそれに基づいて生成された鍵および前記第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項11に記載の情報管理方法。

【請求項14】前記第2の記録媒体に格納されている暗号化された所定の情報を、前記第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して、前記所定の領域に格納されている所定の情報を更新する、請求項13に記載の情報管理方法。

【請求項15】前記媒体固有の情報は前記記録媒体から電子的に入手できるとともに可視的に前記記録媒体上に表示されている、請求項1～14にいずれかに記載の情報管理方法。

【請求項16】前記記録媒体を駆動する装置に固有の情報は、前記装置から電子的に入手できるとともに可視的に前記装置上に表示されている、請求項6、9または10に記載の情報管理方法。

【請求項17】前記第2の記録媒体を駆動する装置に固有の情報は、前記装置から電子的に入手できるとともに可視的に前記装置上に表示されている、請求項13または14に記載の情報管理方法。

【請求項18】媒体固有の情報を有し、外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域と、外部からの指令に基づいて制御することが不可能な機密領域とを備え、前記ユーザ利用領域に格納された任意の情報に対する利用権に基づく許諾情報が前記機密領域に格納されている記録媒体の情報を管理する情報管理装置であって、

前記ユーザ利用領域に対して任意の情報を書込・読出を行う書込・読出手段と、前記機密領域に格納されている許諾情報を前記媒体固有の情報またはそれに基づいて生成された鍵により暗号化して前記機密領域外に導出する所定情報導出手段と、を備える情報管理装置。

【請求項19】前記暗号化された許諾情報を、前記書込・読出手段により前記ユーザ利用領域に格納する、請求項18に記載の情報管理装置。

【請求項20】前記ユーザ利用領域に格納されている暗号化された許諾情報を前記媒体固有の情報により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項19に記載の情報管理装置。

【請求項21】装置固有の情報を備え、前記所定情報導出手段は、前記許諾情報を前記媒体固有の情報またはそ

れに基づいて生成された鍵および前記装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項18または19に記載の情報管理装置。

【請求項22】前記ユーザ利用領域に格納されている暗号化された許諾情報を前記装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項21に記載の情報管理装置。

【請求項23】前記所定情報導出手段は、前記暗号化された許諾情報を前記記録媒体とは異なる第2の記録媒体に送出する、請求項18に記載の情報管理装置。

【請求項24】前記第2の記録媒体に格納されている暗号化された許諾情報を前記媒体固有の情報により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項23に記載の情報管理装置。

【請求項25】前記第2の記録媒体を駆動する装置は装置固有の情報を備え、前記所定情報導出手段は、前記許諾情報を前記媒体固有の情報またはそれに基づいて生成された鍵および前記第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化する、請求項23に記載の情報管理装置。

【請求項26】前記第2の記録媒体に格納されている暗号化された許諾情報を、前記第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および前記媒体固有の情報またはそれに基づいて生成された鍵により復号化して前記機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える、請求項25に記載の情報管理装置。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、情報管理方法および情報管理装置に関し、特に、媒体固有の情報を有する記録媒体に対して任意の情報を記録・読出を行う際の情報管理方法およびその装置に関する。

##### 【0002】

【従来の技術】コンピュータプログラムなどのソフトウェアや電子出版物では、光磁気ディスク(MO)、デジタルビデオディスク(DVD)、フロッピーディスク(FD)、ミニディスク(MD)、その他の記録媒体上に電子化データを格納して販売される。このような電子化データは、一般にコピーが容易であり、不正コピーが頻繁に行われている。このため、ソフトウェアベンダーや出版者側の著作権が侵害され著しく利益が阻害されるおそれがある。

【0003】このような記録媒体上に格納された電子化データを保護するために、ユーザ固有の情報をを用いて暗号化した許諾情報を生成し、これを記録媒体上の所定の

領域に格納して配布することが提案されている。ソフトウェアや出版物などの電子化データは、所定の暗号鍵によって暗号化されて記録媒体上に格納されている。また、この暗号化された電子化データを復号化するための復号鍵がユーザ固有の情報をを用いて暗号化され、許諾情報として記録媒体上に格納されている。

【0004】ユーザ側では、この許諾情報をユーザ固有の情報により復号化することによって復号鍵を得ることができ、記録媒体上に格納されている暗号化された電子化データをこの復号鍵を用いて復号化して利用することができる。このように構成することによって、ユーザ個々に電子化データの利用権を与える際に、電子化データを暗号化するための暗号鍵を共通にすることができ、ユーザ毎に異なるユーザ固有の情報をを用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

【0005】ここで用いられるユーザ固有の情報とは、例えば、ユーザが使用しているコンピュータまたは記録媒体を駆動する装置に付与されている装置番号である。したがって、ユーザが正規に入手したものであっても、異なる装置では使用できなくなり、この記録媒体を譲渡することもできないという不都合がある。特開平5-257816号公報には、記録媒体にこの媒体固有の情報を与え、暗号化された電子化データを復号するための復号鍵をこの媒体固有の情報により暗号化して記録媒体に格納するようにした方法が提案されている。

【0006】この場合、前述の場合と同様に、電子化データを暗号化する際の暗号鍵を共通にすることができ、ユーザ毎に異なる媒体固有の情報をを用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

##### 【0007】

【発明が解決しようとする課題】上述のような方法においては、暗号化された電子化データは、ユーザがアクセス可能な領域に格納される。また、この電子化データを利用するための許諾情報は、ユーザがアクセス不可能な機密領域に格納される。したがって、正規のユーザであっても許諾情報を読み出してバックアップをとることができず、この機密領域に格納されているデータがなんらかの障害により破壊された場合には、電子化データを利用することができなくなる。このような場合には、ソフトウェアベンダーや出版者、その代理店などの電子化データの管理者による利用権の再発行が必要となる。したがって、この再発行の手続きに煩雑な作業と余分なコストを必要とすることとなる。

【0008】本発明は、記録媒体上に格納された電子化データを利用するために必要な許諾情報がなんらかの障害により破壊された場合であっても、ユーザがバックアップ情報を用いてこれを復帰させることが可能な情報管理方法および情報管理装置を提供することを目的とす

る。

【0009】

【課題を解決するための手段】本発明に係る情報管理方法は、媒体固有の情報を有する記録媒体上の所定の領域に格納された所定の情報を、媒体固有の情報またはそれに基づいて生成された鍵により暗号化して所定の領域外に導出する。ここで、記録媒体は、所定の情報を格納する第1領域と、第1領域と異なる第2領域とを備える構成とすることができる。

【0010】また、第2領域は外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域であり、第1領域は外部からの指令に基づいて制御することが不可能な機密領域で構成することができる。この場合、第2領域に格納される任意の情報は暗号化された電子化データであり、第1領域に格納される所定の情報は電子化データを利用する利用権に基づく許諾情報を含むように構成できる。

【0011】また、所定の情報は、媒体固有の情報またはそれに基づいて生成された鍵により暗号化されて所定の領域に格納される構成とすることができる。さらに、所定の情報は、記録媒体を駆動する装置に固有の情報に基づいて暗号化される構成であってもよい。また、暗号化された所定の情報を第2領域に格納する構成とすることができる。

【0012】この場合、第2領域に格納されている暗号化された所定の情報を媒体固有の情報またはそれに基づいて生成された鍵により復号化し、第1領域に格納されている所定の情報を更新するように構成できる。また、所定の情報を第1領域外に導出する際に、媒体固有の情報またはそれに基づいて生成された鍵および記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。

【0013】この場合には、第2領域に格納されている暗号化された所定の情報を、記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報またはそれに基づいて生成された鍵により復号化して、第1領域に格納されている所定の情報を更新するように構成できる。上述のような構成とすることによって、所定の情報を格納されている所定の領域外に導出する場合には、この媒体に固有の情報により暗号化されているので、他の記録媒体にコピーしても、これを復号化することが困難である。例えば、第2領域にソフトウェアや出版物などの電子化データを格納する際に、この電子化データを暗号鍵により暗号化して格納しておき、これを復号するための復号鍵をこの記録媒体に固有の情報で暗号化してユーザのアクセス不可能な第1領域に格納しておけば、暗号化するための暗号鍵をユーザ個々に変える必要がなく、共通の暗号鍵を用いて暗号化して格納できる。第1領域に格納されている暗号化された復号鍵は、さらに媒体固有の情報を用いて暗号化され

て、第1領域外に導出するように構成しているため、ユーザのバックアップとして保存しておくことが可能である。この保存されたバックアップデータは、媒体固有の情報により暗号化されているため、これを他の記録媒体にコピーしても復号化することが困難であり、電子化データを復号するための復号鍵を得ることは困難である。

【0014】また、所定の領域に格納されている情報が破壊されてもこのバックアップデータに基づいてユーザ側で許諾情報を復元することが可能であり、煩わしい利用権の再発行の手続きを必要としない。また、暗号化された所定の情報を、記録媒体とは異なる第2の記録媒体上に格納するように構成できる。

【0015】この場合、第2の記録媒体に格納されている暗号化された所定の情報を媒体固有の情報またはそれに基づいて生成された鍵により復号化し、所定の領域に格納されている所定の情報を更新するように構成できる。また、所定の情報を第2の記録媒体上に導出する際に、媒体固有の情報またはそれに基づいて生成された鍵および第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。

【0016】この場合には、第2の記録媒体に格納されている暗号化された所定の情報を、第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報またはそれに基づいて生成された鍵により復号化して、所定の領域に格納されている所定の情報を更新するように構成できる。また、媒体固有の情報は記録媒体から電子的に入手できるとともに可視的に記録媒体上に表示されていることが好ましく、記録媒体を駆動する装置に固有の情報および第2の記録媒体を駆動する装置に固有の情報は、装置から電子的に入手できるとともに可視的に装置上に表示されていることが好ましい。

【0017】この場合には、前述したような許諾情報のバックアップデータを第2の記録媒体に保存しておき、第1領域に格納されたデータが破壊されたときに、この第2の記録媒体に格納された情報に基づいて、これを復元することが可能となる。本発明に係る情報管理装置は、媒体固有の情報を有し、外部からの指令に基づいて任意の情報を書込・読出可能なユーザ利用領域と、外部からの指令に基づいて制御することが不可能な機密領域とを備え、ユーザ利用領域に格納された任意の情報に対する利用権に基づく許諾情報が機密領域に格納されている記録媒体の情報を管理する情報管理装置であって、ユーザ利用領域に対して任意の情報を書込・読出を行う書込・読出手段と、機密領域に格納されている許諾情報を媒体固有の情報またはそれに基づいて生成された鍵により暗号化して機密領域外に導出する所定情報導出手段とを備えている。

【0018】ここで、暗号化された許諾情報を、書込・

読出手段によりユーザ利用領域に格納する構成とすることができる。また、ユーザ利用領域に格納されている暗号化された許諾情報を媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【0019】さらに、装置固有の情報を備え、所定情報導出手段は、許諾情報を媒体固有の情報またはそれに基づいて生成された鍵および装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。この場合、ユーザ利用領域に格納されている暗号化された許諾情報を装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【0020】また、所定情報導出手段は、暗号化された許諾情報を記録媒体とは異なる第2の記録媒体に送出するように構成できる。この場合、第2の記録媒体に格納されている暗号化された許諾情報を媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【0021】また、第2の記録媒体を駆動する装置は装置固有の情報を備え、所定情報導出手段は、許諾情報を媒体固有の情報またはそれに基づいて生成された鍵および第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵により暗号化するように構成できる。この場合には、第2の記録媒体に格納されている暗号化された許諾情報を、第2の記録媒体を駆動する装置に固有の情報またはそれに基づいて生成された鍵および媒体固有の情報により復号化して機密領域に格納されている許諾情報を更新する所定情報更新手段をさらに備える構成とすることができる。

【0022】

【発明の実施の形態】本発明の実施形態について図面を参照して説明する。

〔記録媒体〕本発明に用いられる記録媒体は、光磁気ディスク(MO)、デジタルビデオディスク(DVD)、フロッピーディスク(FD)、ミニディスク(MD)、その他のユーザによるデータの書き換えが可能な記録媒体であり、例えば光磁気ディスクについてその記録領域を図1により説明する。

【0023】記録媒体1は、ユーザによる読み出しは可能であるが書き換えが不可能な第1階層2、外部からの指令による読み出し・書き込みが不可能な第2階層3、ユーザが任意に情報の書き込みを行うことが可能な第3階層4を有している。第1階層2には、その媒体について一意に決定される媒体固有番号2が格納されている。第3階層4は、ユーザが任意の情報7を格納することが可能な領域であり、ユーザが利用するためのコンピュータプログラム、電子出版物、その他任意のデータを格納

するユーザコンテンツ領域である。第2階層3は、第3階層4に格納された任意の情報に基づく所定の情報6を格納するための領域であり、たとえば、第3階層4に格納されているコンピュータプログラムや電子出版物などの利用権に基づく許諾情報などが格納される。

〔許諾側の構成〕記録媒体に電子化データを格納して配布する際に、この電子化データを利用するための利用権をユーザ毎に設定する場合、この電子化データを暗号化して記録媒体に格納する。たとえば、図2に示すように、記録媒体11に電子化データを格納する場合、第1階層12に媒体固有番号15、第2階層13に利用権に基づく許諾情報16、第3階層14に暗号化されたコンテンツ17が格納される。ここで、許諾情報16は、ユーザの利用権に基づくデータであり、たとえば暗号化されたコンテンツ17を復号化するための復号鍵とすることができる。

【0024】許諾側のコンピュータ21では、個別鍵生成手段22、許諾情報暗号化手段23、コンテンツ暗号化手段24、暗号鍵テーブル25、復号鍵テーブル26などを備えている。コンテンツ暗号化手段24は、暗号鍵テーブル25の暗号鍵によりコンテンツとなるデータ27を暗号化し、記録媒体11の第3階層14にコンテンツとして格納する。暗号鍵テーブル25の暗号鍵に対応する復号鍵が復号鍵テーブル26に格納される。個別鍵生成手段22は、記録媒体11の第1階層12から読み出した媒体固有番号15をもとに媒体個別鍵を生成する。許諾情報暗号化手段23は、復号鍵テーブル26の復号鍵を媒体個別鍵により暗号化して、記録媒体11の第2階層13に許諾情報16として格納する。

〔ユーザ側の構成〕図1の記録媒体1を駆動するためのユーザ側の駆動装置を図4にその概念構成図として示す。

【0025】駆動装置31は、ユーザ利用領域である第3階層4に任意の情報7の書き込み、読み出しを行う書込・読出手段32と、機密領域である第2階層3に格納されている所定の情報6を第1階層2に格納されている媒体固有番号5を用いて暗号化し第2階層3以外の領域に導出する所定情報導出手段33とを備えている。所定情報導出手段33が許諾情報などの所定の情報を暗号化して導出する場所としては、たとえば、第3階層4または他の記録媒体が考えられる。暗号化した許諾情報を記録媒体1の第3階層4に格納する場合には、書込・読出手段32により任意の情報7として格納させることができる。

【0026】さらに具体的な構成の一例として図4に簡略ブロック図を示す。ユーザ側の駆動装置41は、個別鍵生成手段42、許諾情報復号化手段43、復号鍵格納部44、コンテンツ復号化手段45、復号データ格納部46、許諾情報暗号化手段47などを備えている。個別鍵生成手段42は、記録媒体11の第1階層12に格納

されている媒体固有番号15に基づいて媒体個別鍵を生成するものであって、許諾側の個別鍵生成手段22によって生成される個別鍵と同じものを生成する。許諾情報復号化手段43は、記録媒体11の第2階層13に格納されている許諾情報16を読み出して、個別鍵生成手段42により生成された個別鍵により復号化する。許諾情報復号化手段43によって復号化された許諾情報は、復号鍵格納部44に一時的に格納される。コンテンツ復号化手段45は、記録媒体11の第3階層14に格納されているコンテンツ17を読み出して、復号鍵格納部44に格納されている復号鍵を用いて復号化し、復号データ格納部46に格納するものである。

【0027】許諾情報暗号化手段47は、第2階層13の許諾情報16を読み出して、第1階層12に格納されている媒体固有番号12を用いて暗号化する。この場合、媒体固有番号12をそのまま用いることも可能であり、個別鍵生成手段42によって生成した個別鍵を用いて暗号化することも可能であり、さらに、媒体固有番号12に基づいて暗号鍵を生成しこれを用いて暗号化することも可能である。このあと、暗号化した許諾情報を記録媒体11の第3階層14内に格納する。

〔コンテンツ格納処理〕許諾側において記録媒体11に電子化データを格納する際の動作を図5にフローチャートとして示す。

【0028】ステップS1では、記録媒体11に格納するコンピュータプログラム、電子出版物、その他の電子化データの作成を行う。ステップS2では、電子化データを暗号化するための暗号鍵の作成を行う。ステップS3では、暗号化を行う電子化データと暗号鍵とを対応させて、暗号鍵テーブル25に格納する。このとき同時に、暗号鍵により暗号化されたデータを復号するための復号鍵が作成され、電子化データと復号鍵とを対応させて復号鍵テーブル26に格納する。暗号鍵と復号鍵とを共通のものとし、暗号鍵テーブル25と復号鍵テーブル26とを1つの鍵管理テーブルとすることも可能である。

【0029】ステップS4では、暗号化を行う電子化データに対応する暗号鍵を暗号鍵テーブル25から取り出す。ステップS5では、電子化データを暗号鍵により暗号化する。たとえば、DES暗号を用いる場合には、暗号化を行う電子化データに対して換字とビット転置を繰り返して暗号化を行う。ステップS6では、暗号化された電子化データをコンテンツ17として、記録媒体11の第3階層14に格納する。ステップS7では、暗号化された電子化データの格納が終了したか否かを判別する。暗号化された電子化データの格納がすべて終了した場合には、ステップS8に移行する。

【0030】ステップS8では、記録媒体11の第1階層12から媒体固有番号15を読み出して個別鍵を生成する。ステップS9では、コンテンツ17として記録媒

体11に格納した電子化データに対応する復号鍵を復号鍵テーブル26から読み出して、ステップS8で生成した個別鍵により暗号化する。コンテンツ17として格納した電子化データに対応する復号鍵をすべて暗号化した後、ステップS10において、この暗号化した復号鍵を許諾情報16とし記録媒体11の第2階層13に格納する。

〔電子化データの復号化処理〕記録媒体11の第3階層14に格納されているコンテンツ17は、許諾側が作成した暗号鍵によって暗号化されているため、ユーザ側でこれを利用するためには適切な復号鍵により復号化する必要がある。このときの動作を図6のフローチャートを用いて説明する。記録媒体11が駆動装置41に装着されてデータのロード命令がなされると、ステップS21において、記録媒体11の第1階層12から媒体固有番号15を読み出す。ステップS22では、媒体固有番号15から個別鍵の生成を行う。ここでは、許諾側のステップS8と同じアルゴリズムにより個別鍵を生成する。ステップS23では、記録媒体11の第2階層13に格納されている許諾情報16を読み出してこれをステップS22で生成した個別鍵を用いて復号化する。ここで復号化された許諾情報は、コンテンツ17を復号化するための復号鍵であり、この復号鍵を第3領域14に格納されている電子化データと対応させて復号鍵テーブルとし、これを復号鍵格納部44に一時的に格納する。

【0031】ステップS24では、記録媒体11の第3階層14に格納されているコンテンツ17を読み込む。ステップS25では、復号鍵格納部44に格納されている復号鍵を用いて、読み込んだコンテンツ17を復号化する。ステップS26では、復号化されたコンテンツを実行する。

〔許諾情報のバックアップ処理〕ユーザ側の駆動装置41において、記録媒体11の第2階層13に格納されている許諾情報16はバックアップデータとして保存される。この処理を図7を用いて説明する。

【0032】ステップS31では、記録媒体11の第2階層13に格納されている許諾情報16を読み出す。ステップS32では、読み出した許諾情報16を媒体固有番号15によって暗号化する。このとき、ステップ22により生成された個別鍵を用いて許諾情報16の暗号化を行うことも可能であり、他のアルゴリズムにより媒体固有番号15を暗号化した鍵を用いて暗号化するように構成することも可能である。ステップS33では、暗号化された許諾情報16を記録媒体11の第3階層14内に格納する。

【0033】このような構成の場合、第3階層14内に許諾情報16のバックアップが保存されているため、第2階層13の許諾情報16が破壊されたときに、第3階層14内のバックアップデータを読み出して第2階層13に戻せば、許諾情報16の再発行を待たずにコンテ

ツ17を利用することが可能となる。また、第3階層14に保存されている許諾情報は、媒体固有番号15によって暗号化されているため、記録媒体11の第3階層14に格納されている内容がそっくりコピーされても、元の許諾情報16を復元することは困難であり、コンテンツ17の不正利用を防止することができる。

#### 〔他の実施形態〕

(A) 記録媒体11の第2階層13に格納されている許諾情報16が破壊された場合に、第3階層14に保存しておいた許諾情報のバックアップデータを用いて許諾情報16を復元する機能が、記録媒体11を駆動する駆動装置に備わっている場合について説明する。図8は、このような駆動装置51の制御ブロック図であり、個別鍵生成手段42、許諾情報復号化手段43、復号鍵格納部44、コンテンツ復号化手段45、復号データ格納部46および許諾情報暗号化手段47は、図4に示した実施形態と同様であり説明を省略する。

【0034】許諾情報更新手段52は、記録媒体11の第3階層14に保存されている暗号化された許諾情報を読み出して、これを第1階層12に格納されている媒体固有番号15によって復号化する。ここで、第3階層14に保存されている許諾情報が個別鍵生成手段42によって生成された個別鍵により暗号化されている場合には、復号化に用いる鍵はこの個別鍵を用いることとなる。このあと、復号化された許諾情報は、許諾情報16として記録媒体11の第2階層13に格納される。

【0035】この実施形態の動作について図9にフローチャートとして示す。ステップS41では、記録媒体11の第3階層14に格納されている暗号化された許諾情報を読み出す。ステップS42では、読み出した暗号化された許諾情報を媒体固有番号15によって復号化する。このとき、ステップ22により生成された個別鍵を用いて許諾情報の復号化を行うことも可能であり、他のアルゴリズムにより媒体固有番号15を暗号化した鍵を用いて暗号化されている場合には、この鍵を用いて復号化を行う。ステップS43では、復号化された許諾情報を記録媒体11の第2階層13に許諾情報16として格納する。

【0036】このことにより、記録媒体11の第2階層13に格納されている許諾情報16はなんらかの障害により破壊された場合には、第3階層14にバックアップデータとして保存されている暗号化された許諾情報を用いて復元することが可能である。この復元処理は、駆動装置51内で処理されるため、許諾情報16が外部に出力されることがなく、この情報を不正に利用することは不可能となっている。

(B) 記録媒体11を駆動するための駆動装置に固有の装置固有番号によりさらに暗号化を行う場合の実施形態を図10～図12に示す。

【0037】図10に示すように、駆動装置61におい

て、個別鍵生成手段42、許諾情報復号化手段43、復号鍵格納部44、コンテンツ復号化手段45、復号データ格納部46および許諾情報暗号化手段47は、図4に示した実施形態と同様であり説明を省略する。また、駆動装置61は装置固有番号を格納する装置固有番号格納部62を備えている。さらに、第2許諾情報暗号化手段63を備えている。この第2許諾情報暗号化手段63は、許諾情報暗号化手段47で媒体固有番号15によって暗号化された許諾情報を、さらに装置固有番号によって暗号化するものである。この第2許諾情報暗号化手段63によって暗号化された許諾情報は、記録媒体11の第3階層14内に格納される。

【0038】また、駆動装置61は許諾情報更新手段64を備えている。この許諾情報更新手段64は、記録媒体11の第3階層14に保存されている暗号化された許諾情報を読み出して、これを装置固有番号格納部62に格納されている装置固有番号により復号化する第1許諾情報復元手段65と、第1許諾情報復元手段65が復号化した許諾情報を記録媒体11の第1階層12に格納されている媒体固有番号15によって復号化する第2許諾情報復元手段66とを備えている。復元された許諾情報は、記録媒体11の許諾情報16として第2階層13に格納される。

【0039】記録媒体11に格納されている許諾情報16のバックアップを保存する際には、図11に示す手順で行われる。まず、ステップS51では、記録媒体11の第2階層13に格納されている許諾情報16を読み出す。ステップS52では、読み出した許諾情報16を第1階層12に格納されている媒体固有番号15によって暗号化する。ステップS53では、媒体固有番号15によって暗号化された許諾情報を、装置固有番号格納部62に格納された装置固有番号により暗号化する。このあと、暗号化された許諾情報をステップS54において第3階層14内に格納する。

【0040】記録媒体11に格納されている許諾情報16が破壊された場合には、図12に示す手順で許諾情報の復元を行う。ステップS61では、記録媒体11の第3階層14に格納されている暗号化された許諾情報を読み出す。ステップS62では、読み出した暗号化された許諾情報を装置固有番号により復号化する。ステップS63では、装置固有番号により復号化された許諾情報を媒体固有番号15によって復号化する。ステップS64では、復号化された許諾情報を記録媒体11の第2階層13に許諾情報16として格納する。

【0041】このように構成した場合には、許諾情報16のバックアップデータが媒体固有番号15によって暗号化され、さらに駆動装置61の装置固有番号によって暗号化されているため、データの違法コピーを行っても利用することができず、著作権保護をすることができる。また、記録媒体11の許諾情報16が破壊されたと



しても、この駆動装置61を用いて復元することが可能であり、正規のユーザであれば再発行を待たずにコンテンツの利用が可能となる。

【0042】装置固有番号は、記録媒体11を駆動するための駆動装置61に固有の装置番号としたが、ユーザ側で使用しているコンピュータに固有の装置番号を利用することも可能である。また、許諾情報16のバックアップデータを保存する際に装置固有番号によって暗号化した後、媒体固有番号15によって暗号化して格納することも可能であり、これを復元する場合は媒体固有番号15によって復号化した後に装置固有番号によって復号化することとなる。

(C) 許諾情報16のバックアップデータを他の記録媒体に保存しておくことも可能である。このような実施形態について、図13～図15に基づいて説明する。

【0043】記録媒体11を駆動するための駆動装置71は、第2の記録媒体83を駆動するための駆動装置81と接続されており、媒体間のデータのやりとりが可能となっている。駆動装置81は、たとえば、フロッピーディスクドライブ(FDD)、ハードディスクドライブ(HDD)、ミニディスク(MD)、光磁気ディスク(MO)、デジタルディスクドライブ(DVD)などが採用され、装置固有番号を格納するための装置固有番号格納部82を備えており、この装置固有番号を電子データとして出力することが可能となっている。

【0044】記録媒体11を駆動する駆動装置71において、個別鍵生成手段42、許諾情報復号化手段43、復号鍵格納部44、コンテンツ復号化手段45、復号データ格納部46および許諾情報暗号化手段47は、図4に示した実施形態と同様であり説明を省略する。駆動装置71は、さらに、第2許諾情報暗号化手段72と、許諾情報更新手段73とを備えている。第2許諾情報暗号化手段72は、許諾情報暗号化手段47によって暗号化された許諾情報を、さらに駆動装置81の装置固有番号によって暗号化する。このあと、暗号化された許諾情報を第2の記録媒体83に格納する。

【0045】許諾情報更新手段73は、第2の記録媒体83に保存されている暗号化された許諾情報を読み出して、これを装置固有番号格納部82に格納されている装置固有番号により復号化する第1許諾情報復元手段74と、第1許諾情報復元手段74が復号化した許諾情報を記録媒体11の第1階層12に格納されている媒体固有番号15によって復号化する第2許諾情報復元手段75とを備えている。復元された許諾情報は、記録媒体11の許諾情報16として第2階層13に格納される。

【0046】記録媒体11に格納されている許諾情報16のバックアップを保存する際には、図14に示す手順で行われる。まず、ステップS71では、記録媒体11の第2階層13に格納されている許諾情報16を読み出す。ステップS72では、読み出した許諾情報16を第

1階層12に格納されている媒体固有番号15によって暗号化する。ステップS73では、媒体固有番号15によって暗号化された許諾情報を、第2の記録媒体83を駆動するための駆動装置81の装置固有番号により暗号化する。このあと、暗号化された許諾情報をステップS74において第3階層14内に格納する。

【0047】記録媒体11に格納されている許諾情報16が破壊された場合には、図15に示す手順で許諾情報16の復元処理が行われる。ステップS81では、第2の記録媒体83に格納されている暗号化された許諾情報を読み出す。ステップS82では、読み出した暗号化された許諾情報を第2の記録媒体83を駆動する駆動装置81の装置固有番号により復号化する。ステップS83では、装置固有番号により復号化された許諾情報を媒体固有番号15によって復号化する。ステップS84では、復号化された許諾情報を記録媒体11の第2階層13に許諾情報16として格納する。

【0048】このように構成した場合には、許諾情報16のバックアップデータを記録媒体11と切り離して管理することができ、高いセキュリティを維持することができる。また、複数の記録媒体について、その許諾情報をユーザ側で管理することが可能であり、許諾情報がなんらかの形で破壊されても、ユーザ側で対応することが可能である。ここでも、許諾情報16を暗号化する際に、装置固有番号で暗号化した後、媒体固有番号で暗号化するように構成してもよい。この場合には、これを復元する際には、媒体固有番号で復号化した後に装置固有番号で復号化することとなる。

(D) ケーブルテレビやインターネットなどにおいて暗号化したデータを放送し、これをユーザ側で記録媒体に記録させる場合に、上述のような方法を適用することができる。たとえば、ユーザ側から暗号化データを記録した記録媒体の媒体固有番号を放送局に送信させ、その媒体固有番号で暗号化された復号鍵をユーザに送信する。ユーザ側の装置では、この復号鍵を記録媒体の第2階層の許諾情報として格納する。さらに、この許諾情報を媒体固有番号によって暗号化して第3階層に格納する。

【0049】記録媒体上のコンテンツを利用する場合には、媒体固有番号により許諾情報を復号化して復号鍵を生成し、暗号化されたデータを復号化すればよい。この場合にも、他の記録媒体にコンテンツをそのままコピーしても、許諾情報が媒体固有番号によって暗号化されており、復号化することが困難である。また、バックアップデータを用いて許諾情報を復元することが可能であり、許諾情報が破壊された場合であっても、ユーザ側で復元することが可能である。

【0050】

【発明の効果】本発明によれば、記録媒体の所定の領域に格納された所定の情報を、媒体固有の情報によって暗号化して導出しており、他の記録媒体にコピーしても、



これを復号化することが困難である。例えば、ソフトウェアや出版物などの電子化データを格納する際に、この電子化データを暗号鍵により暗号化して格納しておき、これを復号するための復号鍵をこの記録媒体に固有の情報で暗号化してユーザのアクセス不可能な領域に格納しておけば、暗号化するための暗号鍵をユーザ個々に変える必要がなく、共通の暗号鍵を用いて暗号化して格納できる。暗号化された復号鍵は、さらに媒体固有の情報を用いて暗号化されて、所定の領域外に導出するように構成しているため、ユーザのバックアップとして保存しておくことが可能である。この保存されたバックアップデータは、媒体固有の情報により暗号化されているため、これを他の記録媒体にコピーしても復号化することが困難であり、電子化データを復号するための復号鍵を得ることは困難である。また、ユーザはこのバックアップデータを用いて復号鍵を復元することができるため、データがなんらかの障害が破壊された場合であっても、再発行の手続きを省略することが可能となる。

#### 【図面の簡単な説明】

【図1】本発明に用いられる記録媒体の記録領域を示す概念図。

【図2】許諾側における簡略ブロック図。

【図3】本発明の概念構成図。

【図4】1実施形態の簡略ブロック図。

【図5】コンテンツ格納処理の制御フローチャート。

【図6】復号化処理の制御フローチャート。

【図7】バックアップ処理の制御フローチャート。

【図8】他の実施形態の簡略ブロック図。

【図9】許諾情報更新処理のフローチャート。

【図10】他の実施形態の簡略ブロック図。

【図11】その制御フローチャート。

【図12】その制御フローチャート。

【図13】他の実施形態の簡略ブロック図。

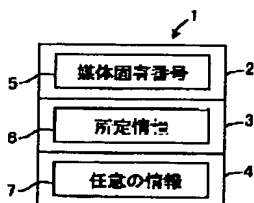
【図14】その制御フローチャート。

【図15】その制御フローチャート。

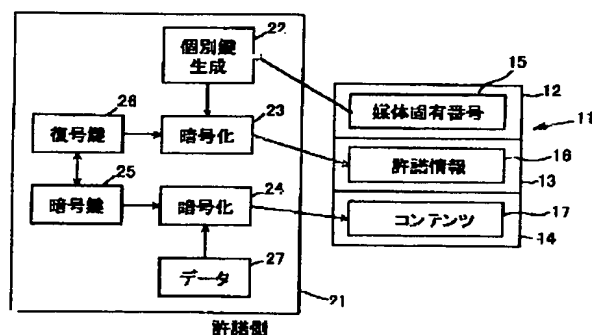
#### 【符号の説明】

- 1 記録媒体
- 2 第1階層
- 3 第2階層
- 4 第3階層
- 5 媒体固有番号
- 6 所定の情報
- 7 任意の情報
- 11 記録媒体
- 12 第1階層
- 13 第2階層
- 14 第3階層
- 15 媒体固有番号
- 16 許諾情報
- 17 コンテンツ
- 21 許諾側コンピュータ
- 22 個別鍵生成手段
- 23 許諾情報暗号化手段
- 24 コンテンツ暗号化手段
- 25 暗号鍵テーブル
- 26 復号鍵テーブル
- 31 駆動装置
- 32 書込・読出手段
- 33 所定情報導出手段
- 41 駆動手段
- 42 個別鍵生成手段
- 43 許諾情報復号化手段
- 44 復号鍵格納部
- 45 コンテンツ復号化手段
- 46 データ格納部
- 47 許諾情報暗号化手段
- 52 許諾情報更新手段
- 83 第2の記録媒体

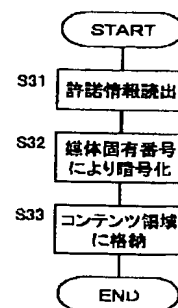
【図1】



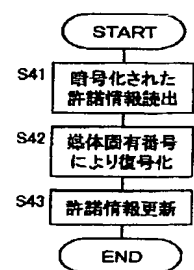
【図2】



【図7】

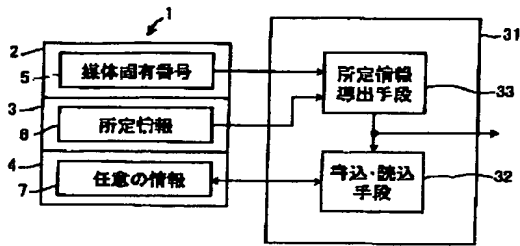


【図9】

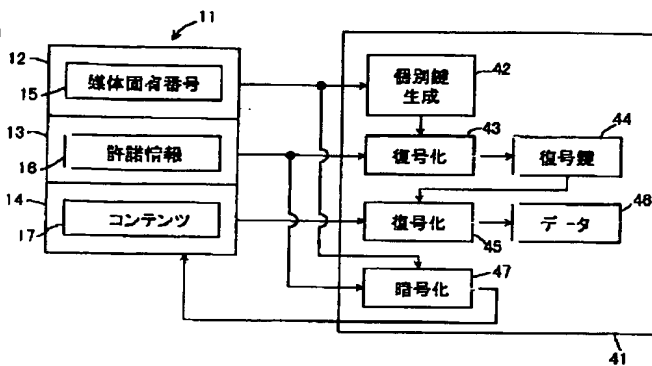


**THIS PAGE BLANK (USPTO)**

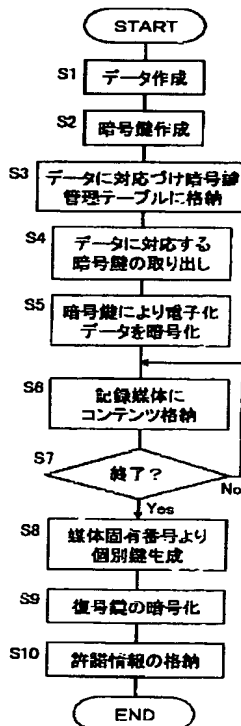
【図3】



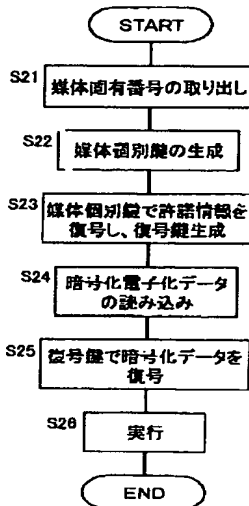
【図4】



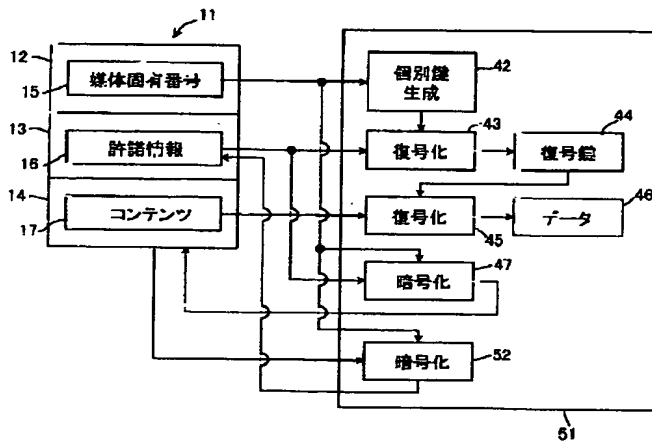
【図5】



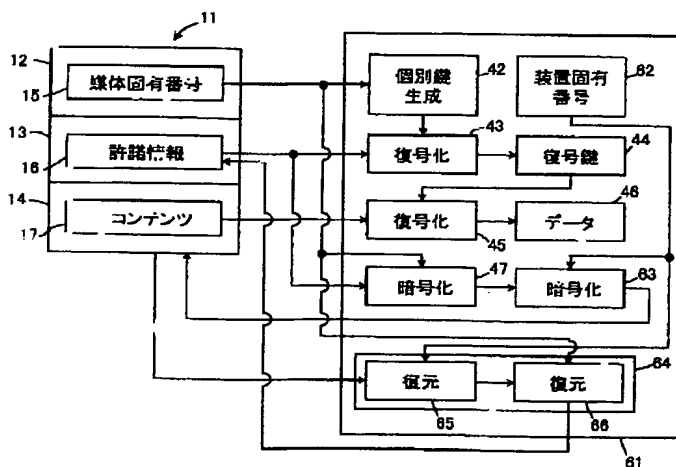
【図6】



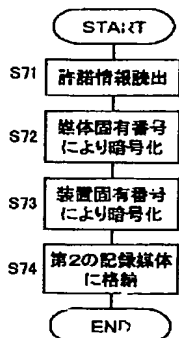
【図8】



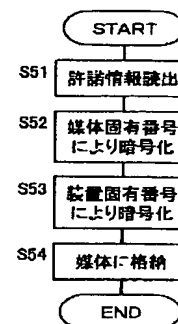
【図10】



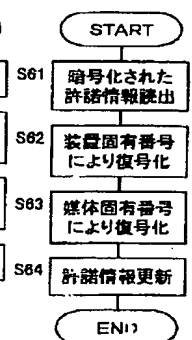
【図14】



【図11】

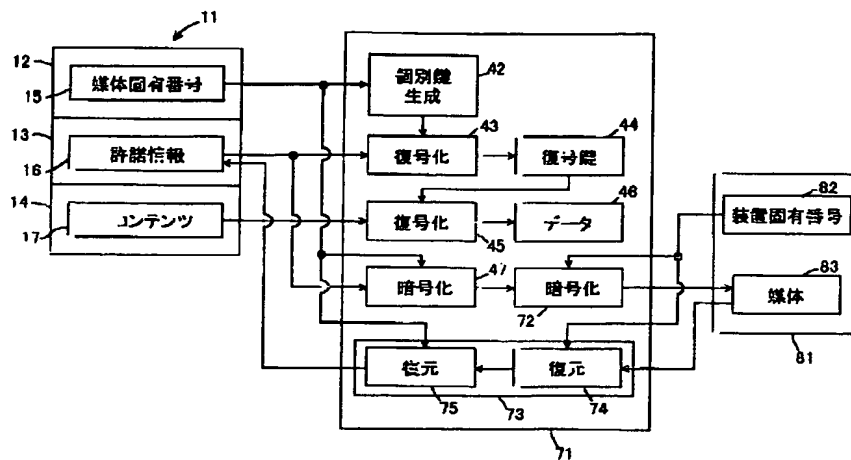


【図12】

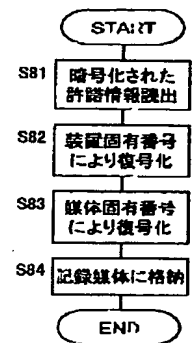


**THIS PAGE BLANK (USPTO)**

【図13】



【図15】



フロントページの続き

(72)発明者 平野 秀幸  
 神奈川県川崎市中原区上小田中4丁目1番  
 1号 富士通株式会社内

Fターム(参考) 5B017 AA07 BA05 BA07 CA15

THIS PAGE BLANK (USPTO)